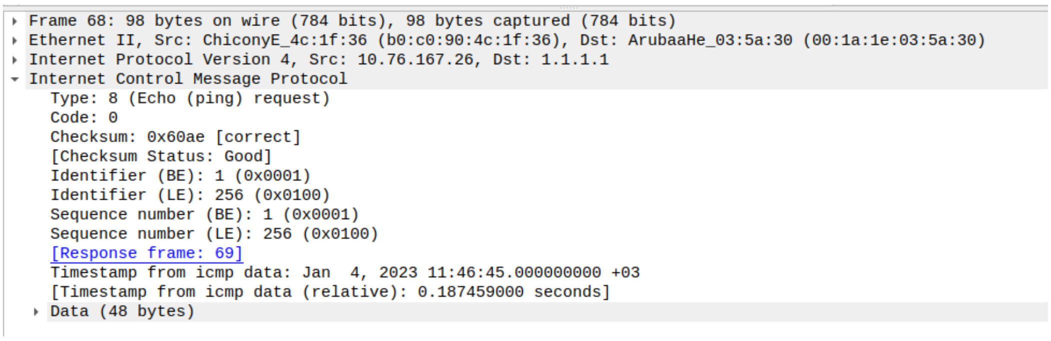
CENG 435
Data Communications and Networking
THE-4

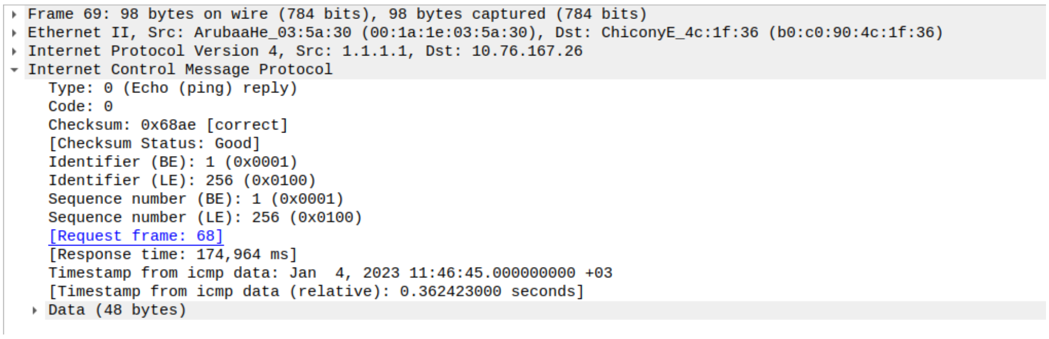
Name: Nihal Taşcı
Id: 2264687

Screenshots



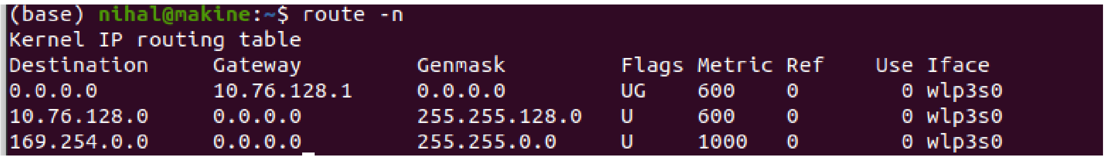
```
▸ Frame 68: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: ChiconyE_4c:1f:36 (b0:c0:90:4c:1f:36), Dst: ArubaaHe_03:5a:30 (00:1a:1e:03:5a:30)
▸ Internet Protocol Version 4, Src: 10.76.167.26, Dst: 1.1.1.1
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x60ae [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 69]
    Timestamp from icmp data: Jan  4, 2023 11:46:45.000000000 +03
    [Timestamp from icmp data (relative): 0.187459000 seconds]
  ▸ Data (48 bytes)
```

Figure 1: ICMP request



```
▸ Frame 69: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: ArubaaHe_03:5a:30 (00:1a:1e:03:5a:30), Dst: ChiconyE_4c:1f:36 (b0:c0:90:4c:1f:36)
▸ Internet Protocol Version 4, Src: 1.1.1.1, Dst: 10.76.167.26
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x68ae [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 68]
    [Response time: 174,964 ms]
    Timestamp from icmp data: Jan  4, 2023 11:46:45.000000000 +03
    [Timestamp from icmp data (relative): 0.362423000 seconds]
  ▸ Data (48 bytes)
```

Figure 2: ICMP response



```
(base) nihal@makine:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.76.128.1     0.0.0.0         UG    600    0        0 wlp3s0
10.76.128.0     0.0.0.0         255.255.128.0   U     600    0        0 wlp3s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp3s0
```

Figure 3: Routing Table

ANSWERS

1.
For ICMP request, the source is 10.76.167.26 and the destination is 1.1.1.1. For ICMP response, the source is 1.1.1.1 and the destination is 10.76.167.26.

2.
On Wireshark, we can see that ICMP protocol uses IP protocol, not UDP or TCP protocol. Because ICMP and IP protocols have no port information, there is no port number in the packet information.

3.
(a) The purpose of the “type” field is declaring the packet type, such as request or response.
(b) The purpose of the “code” field is declaring basic status for request and reply packages, such as network unreachable error.
(c) For type, 8 means ICMP Echo (ping) request, and 0 means ICMP Echo (ping) reply. For code, it is always 0 and it means that there is no problem.

4.
98 bytes, which are 20 bytes for IP header, 14 bytes for Ethernet protocol header, 16 bytes for ICMP header which is 1 byte for declaring, 1 byte for packet code, 2 bytes for checksum, 2 bytes for sequence number and 8 bytes for timestamp data, and 48 bytes for data, are transferred in total by looking at the ICMP request packet information.

5.
For dropping the outgoing packets, the single rule consists of the destination which is 0.0.0.0 and the genmask which is 0.0.0.0 and it should be deleted. Depend on the information from the first question and the routing table, 10.76.128.0 and 169.254.0.0 are private IPs. The target server 1.1.1.1 is only valid for the destination 0.0.0.0 with the genmask 0.0.0.0 because it is a public IP address.

6.
(a) The 48-bit Ethernet address of my computer is b0:c0:90:4c:1f:36.
(b) The 48-bit destination address in the Ethernet frame is 00:1a:1e:03:5a:30. My TP link router belongs to this Ethernet address.